AMENDMENTS TO THE SPECIFICATION

Please replace the paragraph beginning on page 1, line 14, with the following rewritten paragraph:

-- This application claims priority to U.S. Provisional Patent Application No. 60/151,531 entitled "SYSTEM AND METHOD FOR PROVIDING COMPUTER SECURITY" filed August 30, 1999, which is incorporated herein by reference for all purposes. ~~, and to~~ U.S. Patent Application No. 09/615,697 entitled "SYSTEM AND METHOD FOR COMPUTER SECURITY" filed July 14, 2000, ~~which~~ is incorporated herein by reference for all purposes.--

Please replace the paragraph beginning on page 1, line 10, with the following rewritten paragraph:

--This application is related to co-pending U.S. Patent Application No. 09/651,303 ~~No. ______________ (Attorney Docket No. RECOP012~~ entitled EXTENSIBLE INTRUSION DETECTION SYSTEM filed concurrently herewith, which is incorporated herein by reference for all purposes; and co-pending U.S. Patent Application No. 09/651,854 ~~No. ______________ (Attorney Docket No. RECOP013)~~ entitled SYSTEM AND METHOD FOR USING LOGIN CORRELATIONS TO DETECT INTRUSIONS filed concurrently herewith, which is incorporated herein by reference for all purposes; and co-pending U.S. Patent Application No. 09/651,434 ~~No. ______________ (Attorney Docket No. RECOP014)~~ entitled SYSTEM AND METHOD FOR USING SIGNATURES TO DETECT COMPUTER INTRUSIONS filed concurrently herewith, which is incorporated herein by reference for all purposes; and co-pending U.S. Patent Application No. 09/651,304 now U.S. Patent No. 6,647,400 ~~No. ______________ (Attorney Docket No. RECOP015)~~ entitled SYSTEM AND METHOD FOR ANALYZING FILESYSTEMS TO DETECT INTRUSIONS filed concurrently herewith, which is incorporated herein by reference

9/15/05

for all purposes; and co-pending U.S. Patent Application No. 09/651,306, now U.S. Patent No. 6,826,697 ~~No.~~ ____________ ~~(Attorney Docket No. RECOP016)~~ entitled SYSTEM AND METHOD FOR DETECTING BUFFER OVERFLOW ATTACKS filed concurrently herewith, which is incorporated herein by reference for all purposes; and co-pending U.S. Patent Application No. 09/654,347 ~~No.~~ ____________ ~~(Attorney Docket No. RECOP017)~~ entitled SYSTEM AND METHOD FOR USING TIMESTAMPS TO DETECT ATTACKS filed concurrently herewith, which is incorporated herein by reference for all purposes.--

9/15/05
MH

Please replace the paragraph beginning on page 88, line 1, with the following rewritten paragraph:

--Figure 6 illustrates a rule-based system and processes used in some embodiments to detect computer intrusions using a hybrid approach in which both forward chaining and backward chaining are used. Two categories of rule-based systems are those that use *forward-chaining* and those that use *backward-chaining*. Systems that use forward-chaining (602) start with each incoming fact (604) and generate all inferences (606) resulting from the addition of that fact to the knowledge base (608), thereby producing all conclusions that are supported by the available facts. Systems that use backwards-chaining (610) start with a goal (614) and search for facts that support that goal, producing a structure of subgoals (612). Both approaches have the potential for substantial *over-generation*: computing inferences that are never used (forward-chaining) or hypothesizing sub-goals for which there is no support (backward-chaining). The forward- and backward-chaining approaches are analogues of bottom-up and top-down parsing in compiler technology.--

Please replace the paragraph beginning on page 88, line 11, with the following rewritten paragraph:

5. (Original) The system as recited in claim 3, wherein the analysis engine is configured to assign a score to the goal.

6. (Original) The system as recited in claim ~~4~~5, wherein the score comprises at least one of a cost function, a confidence factor, a support value, and importance of the goal.

9/15/05

7. (Canceled)

8. (Previously Presented) The system as recited in claim 5, wherein the analysis engine is further configured to use the scores to select a goal to be pursued.

9. (Original) The system as recited in claim 8, wherein the rules are configured to enable the system to detect an intrusion after occurrence of the intrusion.

10. (Original) The system as recited in claim 9, wherein the rules are configured to cause the analysis engine to correlate and evaluate facts from a plurality of sources of facts.

11. (Original) The system as recited in claim 10, wherein the plurality of sources comprises primary, secondary, and indirect sources of facts.

12. (Original) The system as recited in claim 10, wherein the rules are further configured to cause the analysis to collect, correlate, and evaluate facts related to all phases of an attack.

13. (Original) The system as recited in claim 2, wherein the analysis engine is configured to correlate and evaluate incomplete facts to detect attacks with missing or forged facts.

14. (Original) The system as recited in claim 1, further comprising a user interface, wherein the analysis engine is configured to provide the user interface with an analysis based on the facts and rules, and provide the user interface with information relating to the analysis.

15. (Original) The system as recited in claim 14, wherein the analysis engine is further configured to provide background information relating to the analysis.

16. (Previously Presented) A method implemented on a computer for detecting intrusions on a host, comprising the steps of:

a) providing a source of rules and a source of facts;

b) forward- and backward-chaining using facts from the source of facts and rules from the source of rules by:

(i) using forward chaining to generate one or more inferences: